Data Security: More Reasons to Be On Your Guard

Update prepared by Sally French (Guernsey, Advocate & Senior Associate), Robert Shepherd (Guernsey, Advocate and Partner)
January 2018

// The GDPR and cyber security threats are leading to heightened business vigilance regarding data. A recent case involving Morrisons Supermarket highlights that data threats are not purely external matters, and that the cost of being in business is that you may be held liable for the acts of your employees.

Introduction

We are seeing businesses placing an increased focus on data security and how they manage personal data. With the advent of the GDPR, and complimentary legislation being introduced in Guernsey and Jersey, the timing of this focus is natural. These concerns for businesses have been further heightened by growing publications of cyber security breaches.

In that context, a case marking a worrying combination of data protection and data security issues is the recent UK class action against Morrisons Supermarket. The case has some notable legal and commercial features:

- Commercially;
  - It is a reminder that virtually all businesses hold some personal data. In this instance, the relevant data was employee payroll data.
  - Data security threats can be internal as well as external. The case concerned an intentional data leak perpetrated by a Morrisons' employee.
- Legally
  - The case was the first UK class action for a data security breach. We can expect more.
  - Morrisons were found to be vicariously liable, i.e. though no finding of fault was made against Morrisons it was nevertheless held liable for the acts of its employee.

Headline Facts

The case concerned the leaking of the personal payroll data of almost 100,000 Morrisons' employees. The leak was the result of deliberate, criminal action taken by a disgruntled Morrisons employee, Andrew Skelton. Mr Skelton leaked the data with the intention of damaging Morrisons.

Mr Skelton's role within Morrisons was as an IT auditor. In that role, Mr Skelton legitimately came into possession of the payroll details of over 100,000 Morrisons employees for the purpose of transferring the data from Morrisons secure system to its auditors. Harbouring resentment from an earlier disciplinary incident, Mr Skelton took steps to copy the payroll data onto a personal USB. He took that USB from the workplace and the data on it was leaked some months later using a false account created on a TOR network, accessed from his home computer.

On learning of the leak, Morrisons acted promptly to have the data taken out of public view so far as possible. It offered identity theft protection and compensation to anyone who suffered fraud as a result of the leak. Morrisons incurred costs in the region of £2million as a consequence of the incident.

No point was taken in the case regarding the appropriateness or speed of Morrisons' action. Nevertheless, 5,518 Morrisons employees brought a claim.

Liability

Primary liability claims, seeking to hold Morrisons liable for its own acts and omissions, failed. Morrisons was however held liable on the basis of secondary / vicarious liability. Morrisons was held accountable for the acts of its rogue employee, Mr Skelton.

Vicarious liability sees a faultless party held legally responsible for the wrongs of another. This can arise in a number of relationships, most commonly that of an employer being found liable for the wrongful acts of an employee.

The imposition of vicarious liability on employers is an imperfect compromise. It seeks to balance the social interest of giving victims a remedy against a party with the means to pay, against the risk of unduly inhibiting enterprise with additional costs. The cases show a preference towards the former.

There has been much debate as to how far an employee must stray from the scope of their employment before the chain of liability linking back to their employer will be broken. Criminality is not of itself sufficient to break the link between the employee's acts and the employer's liability. As neatly surmised by Lord Nichols of Birkenhead in Dubai Aluminium Co. Ltd. v Salaam [2003] 2AC 366.

> *"...it is a fact of life, and therefore to be expected by those who carry on businesses, that sometimes their agents may exceed the bounds of their authority or even defy express instructions. It is fair to allocate risk of losses thus arising to the businesses rather than leave those wronged with a sole remedy, of doubtful value, against the individual employee who committed the wrong*."

The test applied by the courts in deciding when an employer is vicariously liable for the act of their employees is whether the wrongful act has a "*sufficiently close connection with the employment*".

The test is imprecise and case specific. As a consequence the courts acknowledge that its parameters are unclear. However, attempts by the courts to over-refine or specify criteria for determining the precise meaning of the term have been resisted. Rather, each case must turn upon its own facts, allowing the courts the latitude to consider the wide range of circumstances to be addressed which will necessarily vary considerably between one matter and another.

On the facts of the *Morrisons* case, Mr Skelton had taken calculated steps with the clear intention of doing his employer harm. His actions were criminal, and he is now serving a prison sentence as a consequence. He was in no way furthering the aims of Morrisons. He had taken data, later leaked it from his own non-work computer, outside of his employer's premises, in non-working hours. Nevertheless, the court concluded that Mr Skelton's rogue actions were sufficiently closely connected with his work to render Morrisons vicariously liable. Drawing upon the earlier criminal judgment against Mr Skelton, the court viewed his actions as "*a seamless and continuous sequence of events*" providing an unbroken thread linking the criminal acts to his employment.

The presiding judge, Mr Justice Langstaff, was troubled that Mr Skelton had set out to injure Morrisons and affixing vicarious liability to Morrisons may render the court an accessory in furthering Mr Skelton's criminal aims. No previous case had gone so far as to hold an employer vicariously liable for acts intended to harm that employer, rather than acts from which the employer may be said to benefit. However when the attack on the employer sees other persons suffer the collateral damage, in this instance having their personal data leaked, it is difficult to see who else might be placed to compensate them. Morrisons do, however, have leave to appeal on this point.

Implications

Widening the scope of vicarious liability may weigh upon any enterprise. The *Morrisons* case is a useful illustration of how the principles may apply in a data protection and data security context. A supermarket may not seem like the most obvious target for a data security attack but the case serves as a reminder that nearly all organisations will hold a quantity of sensitive data.

The case is also notable as having been brought as a class action. The introduction of the GDPR make it easier for such claims to be brought, and provide individuals with a means of seeking redress which it may not be viable for them to obtain acting alone. There is certainly scope for more litigation of this type.

In the context of personal data, given Guernsey's adoption of the GDPR, it can be expected that the courts will uphold the principles underpinning the GDPR. One of the points of that regime is to protect individuals' data privacy. As such, the Guernsey courts would be expected to take a robust approach to see individuals are adequately protected by having access to compensation from an entity which may reasonably be expected to be adequately insured.

The GFSC in its role as regulator would also be expected to carefully scrutinise any breach impacting upon the regulated sector.

Conclusions

Invariably all organisations hold data. Much press attention has been devoted to considering the external threats of data hacks and cyber-attacks. These are serious concerns and organisations should be on their guard against them. But such vigilance against external threats should not divert organisations from considering internal threats. Any system which permits human access to data comes with the enterprise risk that such data may be mis-used, either intentionally or carelessly.

Where the data in question is personal data, the advent of the GDPR provides a valuable opportunity for organisations to review their systems. In doing so organisations should consider:

- What data they hold;
- If they need to hold that data;
- What is the risk of holding that data;
- If they are taking appropriate steps to protect that data from both internal and external risks; and
- If they have a plan to respond in the event that something does go wrong and one of the data risks materialises.

Contacts

Sally French
Advocate & Senior Associate, Guernsey
+44 1481 739 341
sally.french@mourantozannes.com

Robert Shepherd
Advocate & Partner, Guernsey
+44 1481 731 418
robert.shepherd@mourantozannes.com